PCT/JP2004/008056

日本国特許庁 JAPAN PATENT OFFICE

03.06.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年 ６月 ４日

出願番号
Application Number: 特願２００３－１５９９８９

[ST. 10/C]: [ＪＰ２００３－１５９９８９]

出願人
Applicant(s): 松下電器産業株式会社

２００４年 ７月 ８日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特２００４－３０５９０３３

【書類名】　特許願
【整理番号】　2968250019
【あて先】　特許庁長官　　殿
【国際特許分類】　H04L 12/28
【発明者】
　【住所又は居所】　広島県東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内
　【氏名】　森岡　正朋
【発明者】
　【住所又は居所】　広島県東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内
　【氏名】　那須　英正
【発明者】
　【住所又は居所】　広島県東広島市鏡山３丁目１０番１８号　株式会社松下電器情報システム広島研究所内
　【氏名】　杉本　国昭
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100105175
　【弁理士】
　【氏名又は名称】　山広　宗則
　【電話番号】　082-222-9109
【選任した代理人】
　【識別番号】　100105197
　【弁理士】
　【氏名又は名称】　岩本　牧子

【手数料の表示】

【予納台帳番号】　043775

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0215016

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置登録システム、通信装置登録方法及びプログラム

【特許請求の範囲】

【請求項１】通信装置が通信を開始するために、通信相手装置に関する情報の登録を行う通信装置登録システムであって、少なくとも第１の通信装置、第２の通信装置、および、登録情報通信装置を構成要素とし、

前記第１の通信装置は、

前記第２の通信装置との間で、第１の通信路を使用して無線通信を行う第１の通信部と、

前記登録情報通信装置との間で、前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して登録情報を通信する第２の通信部と、

前記登録情報を生成する登録情報生成部と、

前記登録情報を利用して、第２の通信装置を認証する認証部、を備え、

前記第２の通信装置は、

前記第１の通信装置との間で、前記第１の通信路を使用して無線通信を行う第１の通信部と、

前記登録情報通信装置との間で、前記第２の通信路を使用して前記登録情報を通信する第２の通信部と、

前記登録情報を利用して、前記第１の通信装置を認証する認証部、を備え、および、

前記登録情報通信装置は、

前記第２の通信路を使用して、前記第１の通信装置および前記第２の通信装置と通信を行う第２の通信部と、

前記登録情報を記憶する登録情報記憶部、を備えることを特徴とする通信装置登録システム。

【請求項２】前記第２の通信装置用の登録情報を、あらかじめ前記登録情報通信装置および第２の通信装置の記憶部に記録しておくことにより、

前記第１の通信装置の前記登録情報生成部と、

前記第２の通信装置の前記第２の通信部を省略した事を特徴とする請求項１の

通信装置登録システム。

【請求項３】前記登録情報通信装置は、複数の通信装置の登録を可能とするため、前記登録情報を入力する登録情報入力手段を備えたことを特徴とする請求項１又は２に記載の通信装置登録システム。

【請求項４】前記第１の通信装置と、前記第２の通信装置に、前記第１の通信路で通信する情報の暗号化と復号化を行う暗号部をそれぞれ備えることを特徴とする請求項１乃至３のうちいずれか一つに記載の通信装置登録システム。

【請求項５】前記秘匿性の高い第２の通信路は、赤外線通信方式を利用した通信路であることを特徴とする請求項１乃至４のうちいずれか一つに記載の通信装置登録システム。

【請求項６】前記登録情報通信装置は、フレキシブルディスクまたはメモリーカードなどの物理媒体であり、通信装置と直接接続して登録情報を通信することを特徴とする請求項１乃至５のうちいずれか一つに記載の通信装置登録システム。

【請求項７】前記登録情報に、第１の通信装置と第２の通信装置で共有するパスワード及び登録を行う通信装置の機器アドレスを含むことを特徴とする請求項１乃至６のうちいずれか一つに記載の通信装置登録システム。

【請求項８】登録情報通信装置と第１の通信装置と第２の通信装置の間で行う通信方法であって、

前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して、前記登録情報通信装置から前記第１の通信装置へ、登録開始要求を送信するステップと、

前記第１の通信装置において前記登録開始要求を受信するステップと、

前記第１の通信装置において前記登録情報を生成するステップと、

前記第２の通信路を使用して、前記第１の通信装置から前記登録情報通信装置へ、前記生成した登録情報を送信するステップと、

前記登録情報通信装置において、前記登録情報を受信し、記憶するステップと、

前記第２の通信路を使用し、前記登録情報通信装置から前記第２の通信装置に前記登録情報を送信するステップと、

前記第２の通信装置において前記登録情報を受信するステップと、

前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を備えることを特徴とする通信装置登録方法。

【請求項９】登録情報通信装置と第１の通信装置と第２の通信装置の間で行う通信方法であって、

前記登録情報通信装置に記憶している登録情報を、前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して前記第１の通信装置に送信するステップと、

前記第１の通信装置において、前記登録情報を受信するステップと、

前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を備えることを特徴とする通信装置登録方法。

【請求項１０】登録情報通信装置と第１の通信装置と第２の通信装置の間で実行させるためのプログラムであって、

前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して、前記登録情報通信装置から前記第１の通信装置へ、登録開始要求を送信するステップと、

前記第１の通信装置において前記登録開始要求を受信するステップと、

前記第１の通信装置において前記登録情報を生成するステップと、

前記第２の通信路を使用して、前記第１の通信装置から前記登録情報通信装置へ、前記生成した登録情報を送信するステップと、

前記登録情報通信装置において、前記登録情報を受信し、記憶するステップと、

前記第２の通信路を使用して、前記登録情報通信装置から前記第２の通信装置に前記登録情報を送信するステップと、

前記第２の通信装置において前記登録情報を受信するステップと、

前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を実行させることを特徴とするプログラム。

【請求項１１】登録情報通信装置と第１の通信装置と第２の通信装置の間で実行するプログラムであって、

前記登録情報通信装置に記憶している登録情報を、前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して前記第１の通信装置に送信するステップと、

前記第１の通信装置において、前記登録情報を受信するステップと、

前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信装置登録システム、通信装置登録方法およびプログラムに関し、特に、登録情報通信装置を使用することで、簡易に通信装置の登録を実行できるようにした、通信装置登録システム、通信装置登録方法およびプログラムに関する。

【０００２】

【従来の技術】

無線通信システムにおいて、通信相手装置の成りすましや、通信傍受による通信データの漏洩を防ぐための方法として、共通鍵を使用した通信相手装置の認証や通信データの暗号化、復号化などの方法が知られている。

この時、共通鍵の作成方法としては、ユーザーが直接共通鍵を入力する方法や、ユーザーがパスワードまたはパスコード（以下パスワードと総称する）を入力し、乱数や機器アドレスなどを利用して共通鍵を作成する方法などがある。

例えば、２．４５ＧＨｚ帯の電波を使用する近距離無線通信の規格であるＢｌｕｅｔｏｏｔｈ（Ｒ）では、認証用の共通鍵としてリンクキーを使用する。

リンクキーの作成方法としては、ユーザーが直接入力する方法や、ユーザーが入力したＰＩＮコードと呼ばれるパスワードと乱数、機器アドレスから計算により作成する方法などが規定されている。

実際のシステムで考えた場合、通信を行う双方の通信装置に共通鍵やパスワードなどの同じ数値を設定する必要がある。以下では通信相手の通信装置の機器アドレスと共有鍵を記憶する事を登録すると称す。

【０００３】

登録方法としては、図１の様に第１の無線通信装置、第２の無線通信装置共に共通鍵やパスワード、機器アドレスなどの登録情報を入力する手段を内蔵するか、有線で接続できる構成をとり、ユーザーが双方の通信装置に登録情報を入力する方法や、片側の通信装置には登録情報の入力手段を設けず、登録情報を固定しておき、反対側の通信装置で固定の登録情報を入力する方法が一般的である（従来例１）。

【０００４】

またその他に、第１の無線通信装置が壁面上部や天井などのようにユーザーが入力しにくい場所に設置されるため、登録情報入力手段を持たない場合、図２の様に、無線で接続された登録用の無線通信装置を設け、新規に登録する通信装置の登録情報を入力し、暗号化した無線データとして送信する方法もある（従来例２）。

【０００５】

しかし、従来例１及び２では、家電製品などに無線通信機能を搭載する際、各製品への共通鍵やパスワードの入力作業が非常に煩雑であると共に、誤り易いという課題が存在する。

【０００６】

これを解決するため、図３の様に片側の通信装置で固定の登録情報を、初回のみ認証、暗号化していない無線通信路で送信する方法もある（従来例３）。

しかし、従来例３は、認証、暗号化していない無線通信路で登録情報を送信するため、悪意の第３者に登録情報が漏れる可能性があるという課題があった。

【０００７】

これらの課題を解決する技術として、特許公開公報で下記特許文献１が開示されている。この技術は、図４の様に、２台の無線通信装置間で赤外線やセルラー電話など通常の通信路とは別の信頼性の高い通信路を利用して登録情報（特許文

献１ではキー情報と記載）を通信し、双方の機器の認証や暗号化を図るというものである（従来例４）。

【０００８】

【特許文献１】

特開２００３－１８１４８号公報

【０００９】

【発明が解決しようとする課題】

上記特許文献１の技術では、信頼性のある通信路を利用して登録情報を通信することにより、安全に２つの通信装置に登録情報を登録することができる。

しかし、信頼性のある通信路として本来の通信路とは別の通信路を使用する場合、本来の通信路と信頼性のある通信路の通信エリアの違いにより、本来の通信路では通信できるのに、信頼性のある通信路では通信できないエリアが存在するという課題が発生する。例えば、無線ホームネットワークシステムでアクセスポイントを１階に、エアコンを２階に設置するような場合、本来の通信路である無線を使用した通信は可能であるが、信頼性のある赤外線を利用した通信は不可能となる場合である。

また、セルラー電話を使用する場合、登録時にのみ必要なだけで、それ以外では使用しないセルラー電話の通信機能を新たに付け加える必要があり、機器のコストが上がるという課題がある。

【００１０】

本発明は、家庭内の離れた場所に設置した通信装置間で、簡易に、しかも安価に互いの通信装置に関する情報を登録することを目的としている。

【００１１】

【課題を解決するための手段】

この課題を解決するために本発明は、以下に示す特徴を備えている。

第１の発明は、通信装置が通信を開始するために、通信相手装置に関する情報の登録を行う通信装置登録システムであって、少なくとも第１の通信装置、第２の通信装置、および、登録情報通信装置を構成要素とし、

前記第１の通信装置は、前記第２の通信装置との間で、第１の通信路を使用し

て無線通信を行う第１の通信部と、前記登録情報通信装置との間で、前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して登録情報を通信する第２の通信部と、前記登録情報を生成する登録情報生成部と、前記登録情報を利用して、第２の通信装置を認証する認証部、を備え、

前記第２の通信装置は、前記第１の通信装置との間で、前記第１の通信路を使用して無線通信を行う第１の通信部と、前記登録情報通信装置との間で、前記第２の通信路を使用して前記登録情報を通信する第２の通信部と、前記登録情報を利用して、前記第１の通信装置を認証する認証部、を備え、および、

前記登録情報通信装置は、前記第２の通信路を使用して、前記第１の通信装置および前記第２の通信装置と通信を行う第２の通信部と、前記登録情報を記憶する登録情報記憶部、を備えることを特徴とする。

【００１２】

第２の発明は、第１の発明に従属する通信装置登録システムであって、前記第２の通信装置用の登録情報を、あらかじめ前記登録情報通信装置および第２の通信装置の記憶部に記録しておくことにより、前記第１の通信装置の前記登録情報生成部と、前記第２の通信装置の前記第２の通信部を省略した事を特徴とする。

【００１３】

第３の発明は、第１又は２の発明に従属する通信装置登録システムであって、前記登録情報通信装置は、複数の通信装置の登録を可能とするため、前記登録情報を入力する登録情報入力手段を備えたことを特徴とする。

【００１４】

第４の発明は、第１乃至３のうちいずれか一つに記載の発明に従属する通信装置登録システムであって、前記第１の通信装置と、前記第２の通信装置に、前記第１の通信路で通信する情報の暗号化と復号化を行う暗号部をそれぞれ備えることを特徴とする。

【００１５】

第５の発明は、第１乃至４のうちいずれか一つに記載の発明に従属する通信装置登録システムであって、前記秘匿性の高い第２の通信路は、赤外線通信方式を利用した通信路であることを特徴とする。

【００１６】

第６の発明は、第１乃至５のうちいずれか一つに記載の発明に従属する通信装置登録システムであって、前記登録情報通信装置は、フレキシブルディスクまたはメモリーカードなどの物理媒体であり、通信装置と直接接続して登録情報を通信することを特徴とする。

【００１７】

第７の発明は、第１乃至６のうちいずれか一つに記載の発明に従属する通信装置登録システムであって、前記登録情報に、第１の通信装置と第２の通信装置で共有するパスワード及び登録を行う通信装置の機器アドレスを含むことを特徴とする。

【００１８】

第８の発明は、登録情報通信装置と第１の通信装置と第２の通信装置の間で行う通信方法であって、

前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して、前記登録情報通信装置から前記第１の通信装置へ、登録開始要求を送信するステップと、前記第１の通信装置において前記登録開始要求を受信するステップと、前記第１の通信装置において前記登録情報を生成するステップと、前記第２の通信路を使用して、前記第１の通信装置から前記登録情報通信装置へ、前記生成した登録情報を送信するステップと、前記登録情報通信装置において、前記登録情報を受信し、記憶するステップと、前記第２の通信路を使用し、前記登録情報通信装置から前記第２の通信装置に前記登録情報を送信するステップと、前記第２の通信装置において前記登録情報を受信するステップと、前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を備えることを特徴とする。

【００１９】

第９の発明は、登録情報通信装置と第１の通信装置と第２の通信装置の間で行う通信方法であって、

前記登録情報通信装置に記憶している登録情報を、前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して前記第１の通信装置に送信するステップと

、前記第１の通信装置において、前記登録情報を受信するステップと、前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を備えることを特徴とする。

【００２０】

第１０の発明は、登録情報通信装置と第１の通信装置と第２の通信装置の間で実行させるためのプログラムであって、

前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して、前記登録情報通信装置から前記第１の通信装置へ、登録開始要求を送信するステップと、前記第１の通信装置において前記登録開始要求を受信するステップと、前記第１の通信装置において前記登録情報を生成するステップと、前記第２の通信路を使用して、前記第１の通信装置から前記登録情報通信装置へ、前記生成した登録情報を送信するステップと、前記登録情報通信装置において、前記登録情報を受信し、記憶するステップと、前記第２の通信路を使用して、前記登録情報通信装置から前記第２の通信装置に前記登録情報を送信するステップと、前記第２の通信装置において前記登録情報を受信するステップと、前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を実行させることを特徴とする。

【００２１】

第１１の発明は、登録情報通信装置と第１の通信装置と第２の通信装置の間で実行させるためのプログラムであって、

前記登録情報通信装置に記憶している登録情報を、前記第１の通信路に比べて秘匿性の高い第２の通信路を使用して前記第１の通信装置に送信するステップと、前記第１の通信装置において、前記登録情報を受信するステップと、前記受信した登録情報を利用して、前記第１の通信装置と前記第２の通信装置が通信相手装置の認証を行うステップ、を実行させることを特徴とする。

【００２２】

【発明の実施の形態】

以下、本発明の実施の形態について、図５から図１０を用いて説明する。

なお、実施の形態は、無線ホームネットワークに新たに無線通信対応の家電製

品を登録する際、本発明を適用した例とする。

【００２３】

（第１の実施形態）

図５は、本発明の第１の実施形態に係るシステム構成図である。また、図７はアクセスポイント（第１の通信装置）５０１、エアコン（第２の通信装置）５０４、および双方向赤外線リモコン（登録情報通信装置）５０５間のシーケンス図である。

図５において、アクセスポイント５０１（第１の通信装置）は１階の壁面上部に、テレビ５０２および冷蔵庫５０３は１階床面に設置してある。

アクセスポイント５０１は、無線ホームネットワークの基地局の役割を持っており、テレビ５０２からアクセスポイント５０１を介して冷蔵庫５０３の情報を取得するなど、各機器はアクセスポイント５０１と通信することにより無線ホームネットワークに接続している。

【００２４】

ここで、ユーザーは新たにエアコン５０４（第２の通信装置）を購入し、２階の壁面上部に設置したとする。新たに設置したエアコン５０４を無線ホームネットワークに接続するためには、アクセスポイント５０１とエアコン５０４の両機器が、機器認証やデータの暗号化、復号化で使用する共有鍵を持つ必要がある。

両機器に共有鍵を設定するために、ユーザーは以下の手順で作業を行う。

まず、５０５－１の位置から双方向赤外線リモコン（登録情報通信装置）５０５をアクセスポイント５０１に向け、双方向赤外線リモコン５０５の登録開始ボタンを押す。すると、双方向赤外線リモコン５０５からアクセスポイント５０１に赤外線で登録開始要求が送られる（７００）。

登録開始要求を受信したアクセスポイント５０１は、共有鍵を作成するために使用するパスワードとして新たに生成した乱数と、アクセスポイント５０１の機器アドレスを登録情報として双方向赤外線リモコン５０５に赤外線で送信し（７０１）、接続待ち状態になる。

双方向赤外線リモコン５０５は赤外線により受信した登録情報を記憶する。

【００２５】

次にユーザーは双方向赤外線リモコン５０５を持って、エアコン５０４と赤外線で通信できる５０５－２の位置まで移動し、双方向赤外線リモコン５０５をエアコン５０４に向けて登録情報送信ボタンを押す。すると、双方向赤外線リモコン５０５からエアコン５０４に向けて、記憶していた登録情報（パスワードとアクセスポイント５０１の機器アドレス）が赤外線で送信される（７０２）。

登録情報を受信したエアコン５０４は、受信した機器アドレスを使用してアクセスポイント５０１に接続を行い（７０３）、アクセスポイント５０１とエアコン５０４の間で、パスワード、機器アドレス及び無線で伝送する乱数から機器認証用の共有鍵（以下認証鍵と略す）を作成し、相互に通信相手機器が正しい機器であることを認証（以下相互認証と略す）する（７０４）。作成した認証鍵はこれ以降無線接続を行う際に使用し、無線接続を行うたびに相互認証を行う。

また、この時、認証鍵と無線で伝送する乱数から暗号化、復号化用の共有鍵（以下暗号鍵と略す）も作成する（７０５）。これ以降、アクセスポイント５０１とエアコン５０４の間のデータ通信（７０６）は暗号鍵を使用して、暗号化、復号化を行う。

【００２６】

次に、図６、図７を使用して、詳細な動作について説明する。

まず、ユーザーは双方向赤外線リモコン５０５をアクセスポイント５０１に向け双方向赤外線リモコン５０５の登録開始ボタンを押すことにより、登録開始要求送信手段６２０を起動する。登録開始要求送信手段６２０は、第１の通信路である無線通信路よりも秘匿性の高い、第２の通信路たる赤外線で登録開始要求をアクセスポイント５０１に送信する（７００）。

登録開始要求受信手段（第２の通信部）６０５により、登録開始要求を受信したアクセスポイント５０１は、登録情報送信手段（第２の通信部）４００により、共有鍵を作成するために使用するパスワードとして新たに生成した乱数と、アクセスポイント５０１の機器アドレスを登録情報として双方向赤外線リモコン５０５に赤外線で送信し（７０１）、無線通信手段（第１の通信部）１０２は接続待ち状態になる。なお、この登録情報の生成は、アクセスポイント５０１の登録情報送信手段４００内に設けられた生成手段（図示を省略）で行われる。

双方向赤外線リモコン５０５は登録情報受信手段６２１により受信した登録情報を、登録情報記憶手段６２２に記憶する。

【００２７】

次にユーザーは双方向赤外線リモコン５０５を持って、エアコン５０４と赤外線で通信できる位置まで移動し、双方向赤外線リモコン５０５をエアコン５０４に向けて登録情報送信ボタンを押すことにより、登録情報送信手段６２３を起動する。すると、双方向赤外線リモコン５０５の登録情報送信手段６２３は、赤外線を使ってエアコン５０４に向け、登録情報記憶手段６２２に記憶していた登録情報（パスワードとアクセスポイント５０１の機器アドレス）を送信する（７０２）。

登録情報受信手段（第２の通信装置の第２の通信部）４１０を使用して登録情報を受信したエアコン５０４は、受信した機器アドレスを使用し、無線通信手段（第２の通信装置の第１の通信部）１１２を使用してアクセスポイント５０１に接続を行う（７０３）。アクセスポイント５０１の認証手段１０１とエアコン５０４の認証手段１１１は、無線通信手段１０２と１１２を介して、パスワード、機器アドレス及び無線で伝送する乱数から認証鍵を作成し、相互認証を行う（７０４）。作成した認証鍵はこれ以降無線接続を行う際に使用し、無線接続を行うたびに相互認証を行う。

また、この時、暗号手段１０３と１１３は、認証鍵と無線で伝送する乱数から暗号鍵も作成する（７０５）。これ以降、アクセスポイント５０１とエアコン５０４の間のデータ通信（７０６）は暗号鍵を使用して、暗号化、復号化を行う。

【００２８】

以上のように、ユーザーは新たにエアコンを設置した時に、双方向赤外線リモコン５０５をアクセスポイント５０１に向けて１回ボタンを押し、次にエアコン５０４の場所まで移動してエアコン５０４に向け１回ボタンを押すだけの動作で、エアコン５０４を簡単に無線ホームネットワークに接続することが出来、暗号化により他人に傍受されること無く安全にデータ通信を行うことが出来る。

なお、無線通信方式として、Ｂｌｕｅｔｏｏｔｈ（Ｒ）、ＩＥＥＥ８０２．１１、ＥＣＨＯＮＥＴの小電力無線が使用できることは言うまでもない。

また、赤外線通信方式として、赤外線リモコン、ＩｒＤＡ方式が使用できることは言うまでもない。

また、双方向赤外線リモコン５０５の記憶領域を節約するため、アクセスポイント５０１から双方向赤外線リモコン５０５を介してエアコン５０４に送る登録情報にアクセスポイント５０１の機器アドレスを含めない場合でも、エアコン５０４が通信可能な機器の発見動作を行い、通信可能な機器に順番に接続して相互認証が可能か試みることにより、アクセスポイント５０１と相互認証が可能であることは言うまでもない。

また、アクセスポイント５０１は登録開始要求を受け取る、受け取らないに関わらず、常に接続待ち状態に出来ることは言うまでもない。

【００２９】

また、アクセスポイント５０１やエアコン５０４の記憶容量および処理負荷削減のため、登録情報としてパスワードではなく、共有鍵を使用することが可能であることは言うまでもない。

また、無線通信するデータが暗号化する必要のないデータである場合、機器の処理負荷を低減し、より安価なハードウェアで無線ホームネットワークへのアクセスを実現するため、暗号鍵の作成、および無線通信データの暗号化、復号化を行わない構成が可能であることは言うまでもない。

また、双方向赤外線リモコンの代わりに、赤外線通信機能付きの携帯電話やコンピュータが使用できることは言うまでもない。

また、アクセスポイント５０１の消費電力低減およびハードウェア簡易化のため、アクセスポイント５０１に赤外線受信手段を設けず、代わりにボタンなどの登録開始手段を設け、双方向赤外線リモコン５０５からアクセスポイント５０１への赤外線による登録開始要求送受信を省略できることは言うまでもない。

【００３０】

（第２の実施形態）

図８は、本発明の第２の実施形態に係るシステム構成図である。また、図１０はアクセスポイント（第１の通信装置）５０１、防犯センサー（第２の通信装置）８０１、記録媒体（登録情報通信装置）８０２間のシーケンス図である。

図８において、第１の実施形態同様、アクセスポイント（第１の通信装置）５０１は１階の壁面上部に、テレビ５０２および冷蔵庫５０３は１階床面に設置してある。

第１の実施形態同様、アクセスポイント５０１は、無線ホームネットワークの基地局の役割を持っており、テレビ５０２からアクセスポイント５０１を介して冷蔵庫５０３の情報を取得するなど、各機器はアクセスポイント５０１と通信することにより無線ホームネットワークに接続している。

【００３１】

ここで、ユーザーは新たに電池駆動の防犯センサー（第２の通信装置）８０１を購入し、１階の屋外の壁面上部に設置したとする。

新たに設置した防犯センサー８０１を無線ホームネットワークに接続するためには、アクセスポイント５０１と防犯センサー８０１の両機器が機器認証とデータの暗号化、復号化で使用する共有鍵を持つ必要がある。

しかし、電池駆動の防犯センサー８０１は、消費電力低減及び小型化のため赤外線通信手段は持っていないため、ユーザーは以下の手順で作業を行う。

ユーザーは、防犯センサー８０１に電池を挿入するもしくは電源スイッチをＯＮにすることにより、防犯センサー８０１の電源をＯＮにする。電源がＯＮになると、防犯センサー８０１は接続待ち状態になる。

【００３２】

次にユーザーは、防犯センサー８０１と一緒に販売している、防犯センサー８０１の登録情報（パスワードと防犯センサー８０１の機器アドレス）を記録してあるフレキシブルディスクやメモリーカード等の記録媒体（登録情報通信装置）８０２を、アクセスポイント５０１に内蔵した読取装置に接続する。

アクセスポイント５０１は、記録媒体８０２が接続されたことを認識すると、記録媒体から登録情報を読み取り（１０００）、受信した防犯センサー８０１の機器アドレスを使用して防犯センサー８０１に接続を行い（１００１）、アクセスポイント５０１と防犯センサー８０１の間で、パスワード、機器アドレス及び無線で伝送する乱数から認証鍵を作成し、相互認証を行う（１００２）。作成した認証鍵はこれ以降無線接続を行う際に使用し、無線接続を行うたびに相互認証

を行う。

またこの時、認証鍵と無線で伝送する乱数から暗号鍵も作成する（１００３）。これ以降、アクセスポイント５０１と防犯センサー８０１の間のデータ通信（１００４）は暗号鍵を使用して、暗号化、復号化を行う。

【００３３】

次に、図９，図１０を使用して、詳細な動作について説明する。

ユーザーは、防犯センサー８０１に電池を挿入するもしくは電源スイッチをＯＮにすることにより、防犯センサー８０１の電源をＯＮにする。電源がＯＮになると、防犯センサー８０１の無線通信手段１１２は接続待ち状態になる。

次にユーザーは、防犯センサー８０１と一緒に販売している、防犯センサー８０１の登録情報（パスワードと防犯センサー８０１の機器アドレス）を記録してあるフレキシブルディスクやメモリーカード等の記録媒体８０２を、アクセスポイント５０１と接続する。アクセスポイント５０１は記録媒体８０２が接続されたことを認識すると、記憶媒体の登録情報送信手段９２１とアクセスポイント５０１の登録情報受信手段９００を利用して登録情報を読み取り（１０００）、読み取った防犯センサー８０１の機器アドレスを使用し、無線通信手段１０２を使用して防犯センサー８０１に接続を行う（１００１）。アクセスポイント５０１の認証手段１０１と防犯センサー８０１の認証手段１１１は、無線通信手段１０２と１１２を介して、パスワード、機器アドレス及び無線で伝送する乱数から認証鍵を作成し、相互認証を行う（１００２）。作成した認証鍵はこれ以降無線接続を行う際に使用し、無線接続を行うたびに相互認証を行う。

また、この時、暗号手段１０３と１１３は、認証鍵と無線で伝送する乱数から暗号鍵も作成する（１００３）。これ以降、アクセスポイント５０１と防犯センサー８０１の間のデータ通信（１００４）は暗号鍵を使用して、暗号化、復号化を行う。

【００３４】

以上のように、ユーザーは新たに防犯センサー８０１を設置した時に、防犯センサー８０１と一緒に販売していた記録媒体をアクセスポイント５０１に接続するだけの動作で、防犯センサー８０１を簡単に無線ホームネットワークに登録す

ることが出来、暗号化により他人から傍受されること無く安全にデータ通信を行うことが出来る。

【００３５】

なお、無線通信方式として、Ｂｌｕｅｔｏｏｔｈ（Ｒ）、ＩＥＥＥ８０２．１１、ＥＣＨＯＮＥＴの小電力無線が使用できることは言うまでもない。

また、記録媒体として、ＣＤやＩＣカード、バーコード、赤外線リモコンなど他の媒体が使用できることは言うまでもない。

また、記録媒体は防犯センサーと一緒に販売しているものではなく、ユーザー所有の記録媒体を防犯センサー販売店に持ち込み記録してもらう形態をとることが可能であることは言うまでもない。

また、記録媒体は、赤外線リモコンや赤外線機能付き携帯電話等のように、ボタンなどのユーザー入力手段を備えている、もしくはフレキシブルディスクやメモリーカードなど、コンピューターなどの電子機器から書き換え可能な記録媒体を使用することで、ユーザーが登録情報を入力することにより、複数の機器の登録に使用できる形態をとることが可能であることは言うまでもない。

【００３６】

【発明の効果】

以上のように本発明によれば、ユーザーは新たに無線ホームネットワーク対応の機器を設置した際に、登録情報通信装置を既設の第１の通信装置に向けて登録開始要求送信手段を起動し、次に新設の第２の通信装置の場所まで移動して第２の通信装置に向け登録情報送信手段を起動するだけの動作で、新設の第２の通信装置を簡単に第１の通信装置に登録することが出来、暗号化により他人に傍受されること無く安全にデータ通信を行うことが出来るという効果が得られる。

【００３７】

また、本発明によれば、ユーザーが新たに登録情報通信装置との通信手段を持たない、無線ホームネットワーク対応の機器を設置した際でも、ユーザーはあらかじめ登録情報を記憶している登録情報通信装置を既設の第１の通信装置と接続するだけの動作で、新設の第２の通信装置を既設の第１の通信装置に登録することが出来るという効果が得られる。

【００３８】

また、本発明によれば、登録情報の送受信には電波に比べて赤外線や電気的接続などの秘匿性の高い通信路を使用することで、パスワードや機器アドレスなどの登録情報が他人に傍受される可能性は非常に低くなる上、認証鍵及び暗号鍵などの共有鍵を作成する際、パスワードに加え乱数を使用することで、送受信するパスワードとは異なる共有鍵を作成するため、共有鍵が悪意の第３者に漏れる可能性は非常に低く、悪意の第３者による成りすましや通信の傍受が防げ、安全にデータ通信を行うことが出来るという効果が得られる。

【図面の簡単な説明】

【図１】

従来の、双方の機器でユーザーが登録情報を入力することで登録を行う際の構成図である（従来例１）。

【図２】

従来の、登録用無線通信端末を利用して登録を行う際の構成図である（従来例２）。

【図３】

従来の、登録情報を無線伝送して登録を行う際の構成図である（従来例３）。

【図４】

従来の、登録情報を信頼性の高い伝送路を利用して伝送し、登録を行う際の構成図である（従来例４）。

【図５】

本発明の第１の実施形態に係るシステム構成図である。

【図６】

本発明の第１の実施形態に係る構成図である。

【図７】

本発明の第１の実施形態に係るシーケンス図である。

【図８】

本発明の第２の実施形態に係るシステム構成図である。

【図９】

本発明の第２の実施形態に係る構成図である。

【図１０】

本発明の第２の実施形態に係るシーケンス図である。

【符号の説明】

１００、１１０、２２０　登録情報入力手段

１０１、１１１、２２１　認証手段

１０２、１１２、２２２　無線通信手段

１０３、１１３、２２３　暗号手段

１０４、１１４、２２４　無線データ利用手段

２００、２１０、６２２、９１０、９２０　登録情報記憶手段

４００、６２３、９２１　登録情報送信手段

４１０、６２１、９００　登録情報受信手段

５０１　アクセスポイント

５０２　テレビ

５０３　冷蔵庫

５０４　エアコン

５０５、５０５－１、５０５－２　双方向赤外線リモコン

６０５　登録開始要求受信手段

６２０　登録開始要求送信手段

７００　登録開始要求

７０１、７０２、１０００　登録情報

７０３、１００１　接続

７０４、１００２　相互認証

７０５、１００３　暗号鍵生成

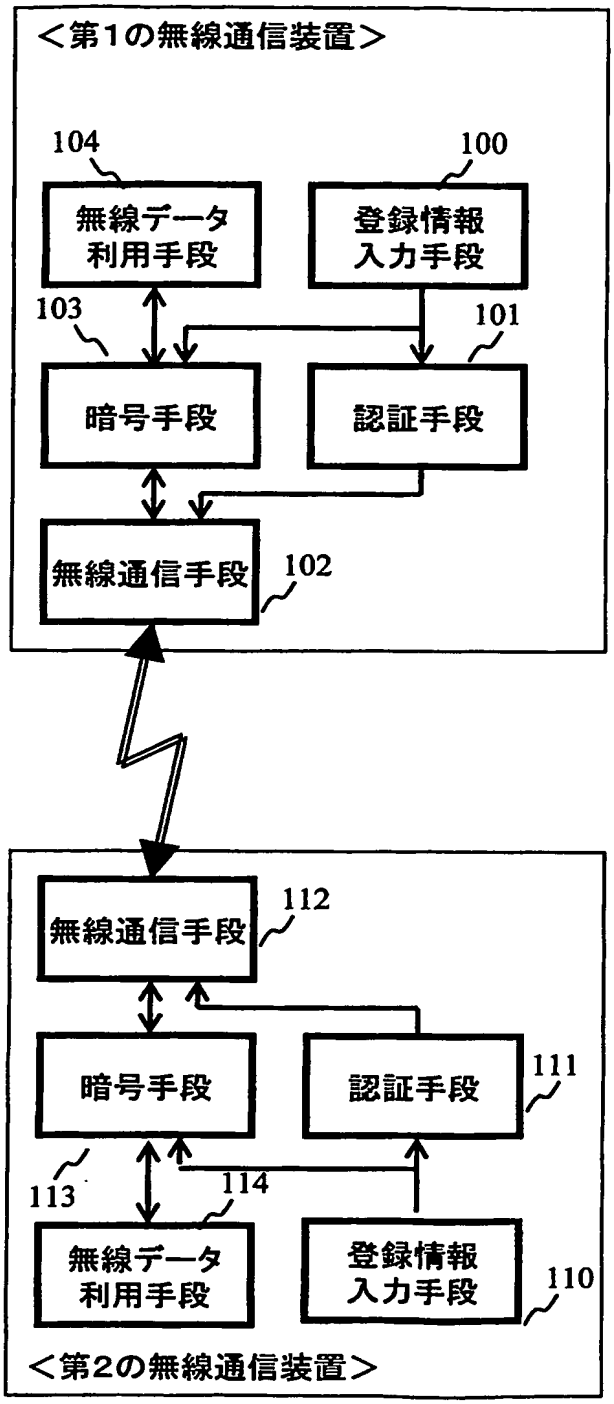
７０６、１００４　データ通信

８０１　防犯センサー

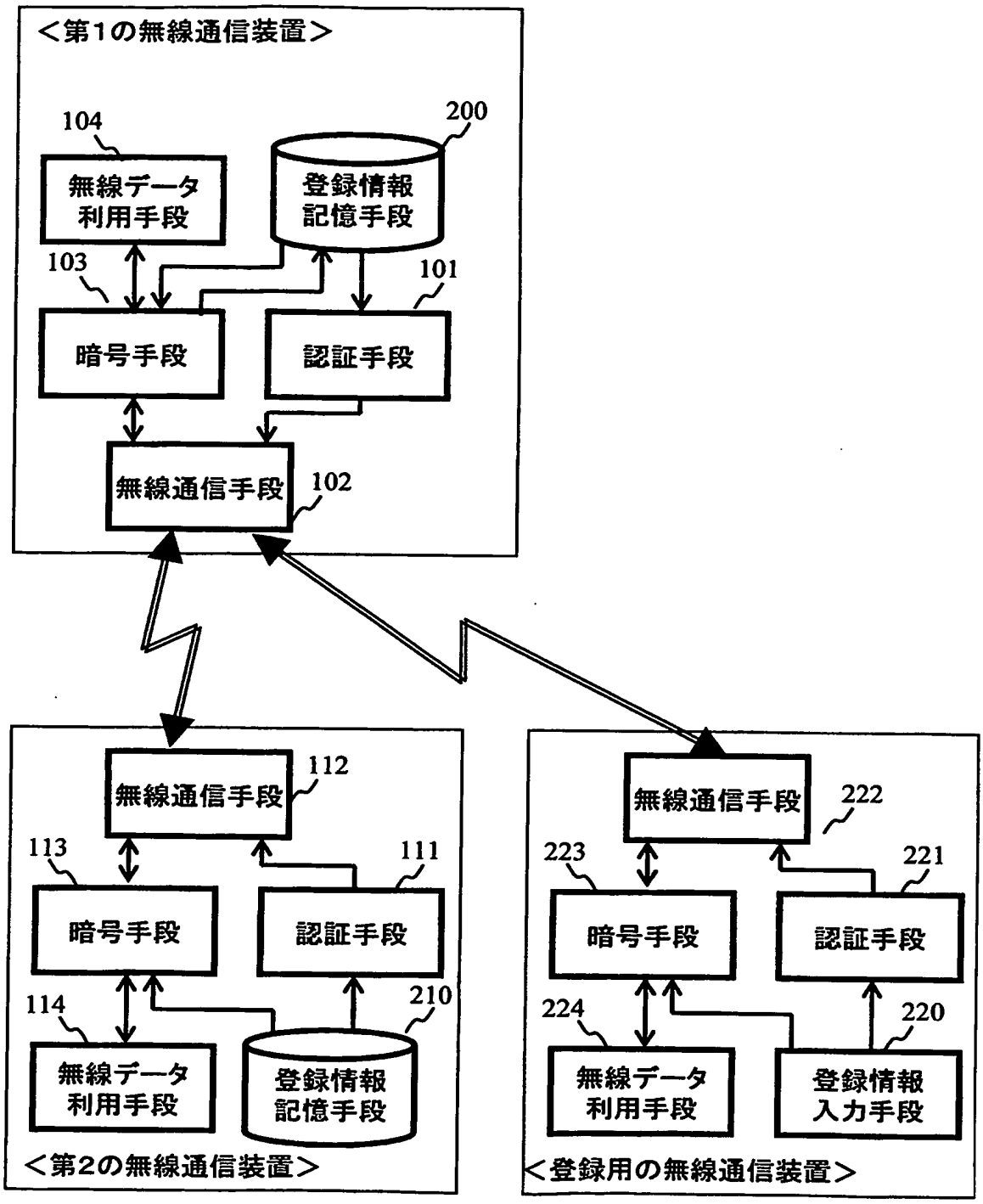
８０２　記録媒体

【書類名】　図面

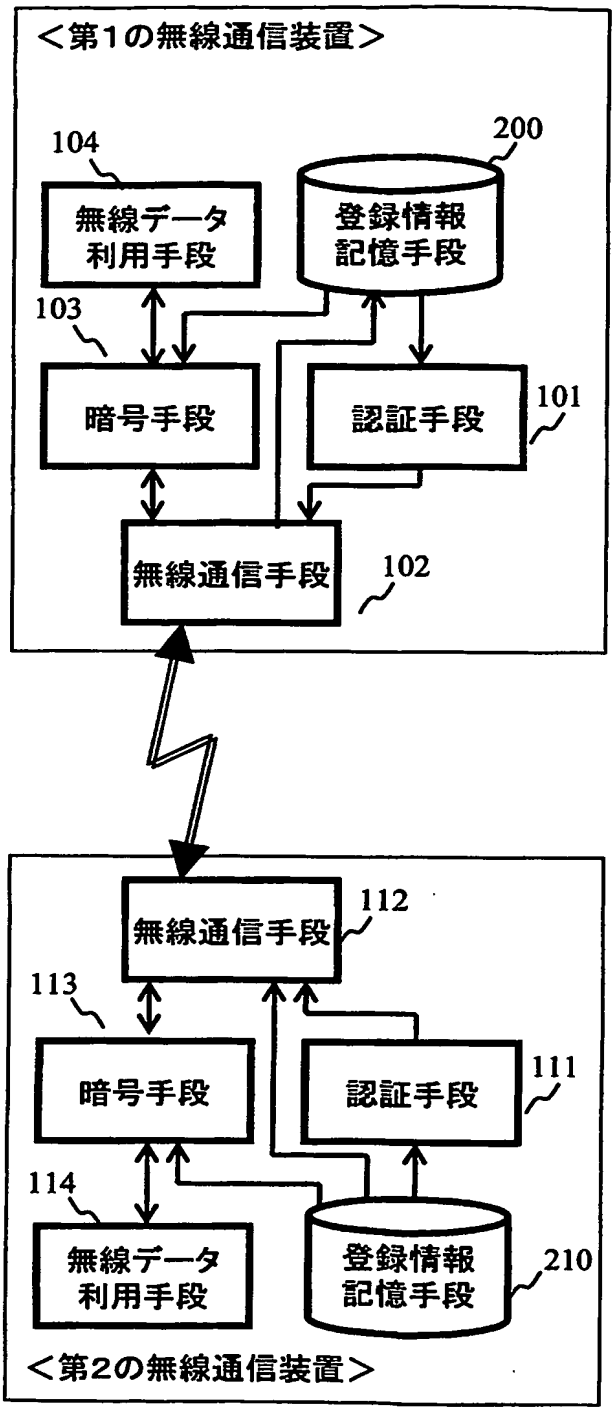
【図１】


<第1の無線通信装置>
104
100
無線データ利用手段
登録情報入力手段
103
101
暗号手段
認証手段
無線通信手段
102
112
無線通信手段
暗号手段
認証手段
111
113
114
無線データ利用手段
登録情報入力手段
110
<第2の無線通信装置>

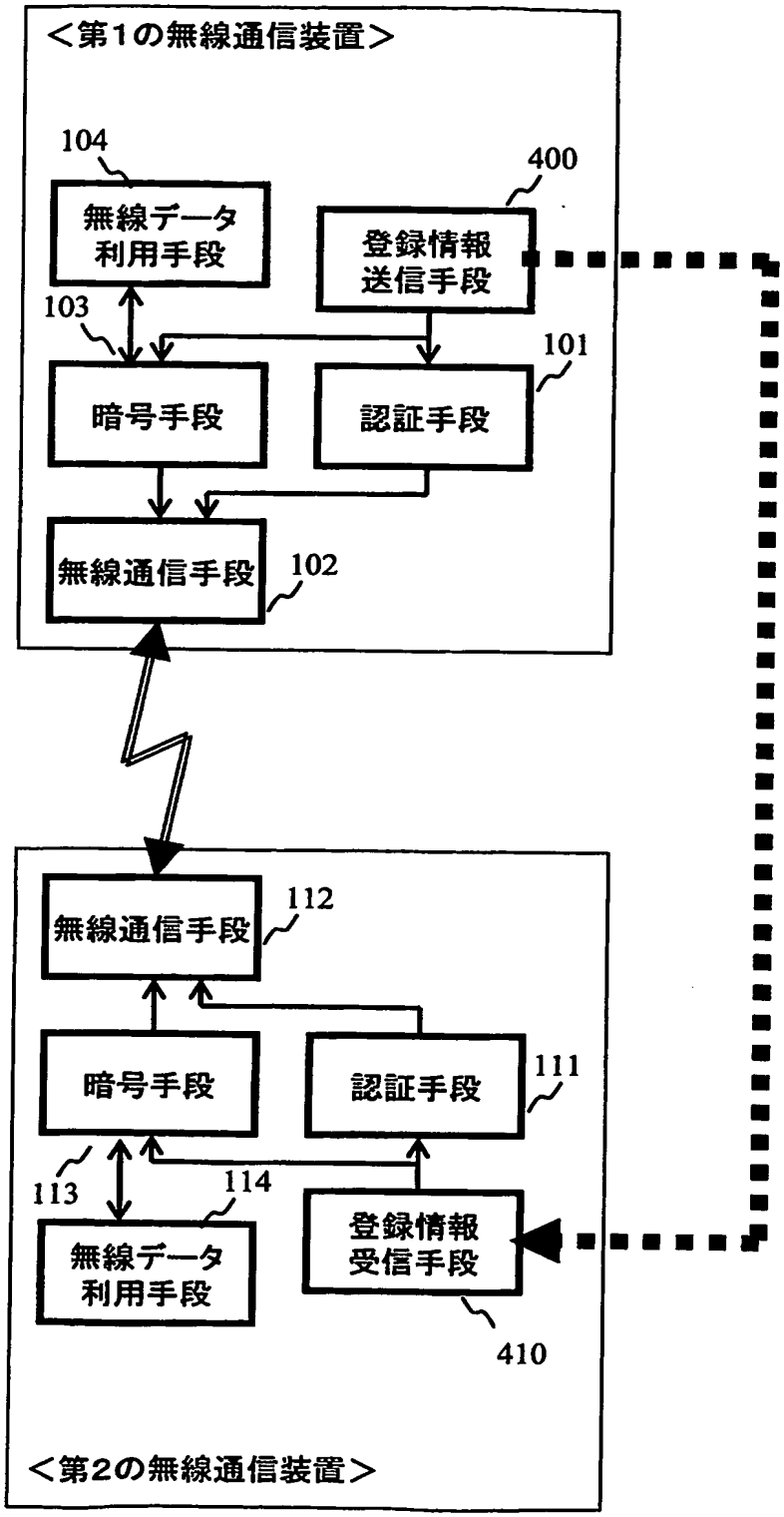
【図２】


<第1の無線通信装置>
104
200
無線データ利用手段
登録情報記憶手段
103
101
暗号手段
認証手段
無線通信手段
102
112
無線通信手段
113
111
暗号手段
認証手段
114
210
無線データ利用手段
登録情報記憶手段
<第2の無線通信装置>
222
無線通信手段
223
221
暗号手段
認証手段
224
220
無線データ利用手段
登録情報入力手段
<登録用の無線通信装置>

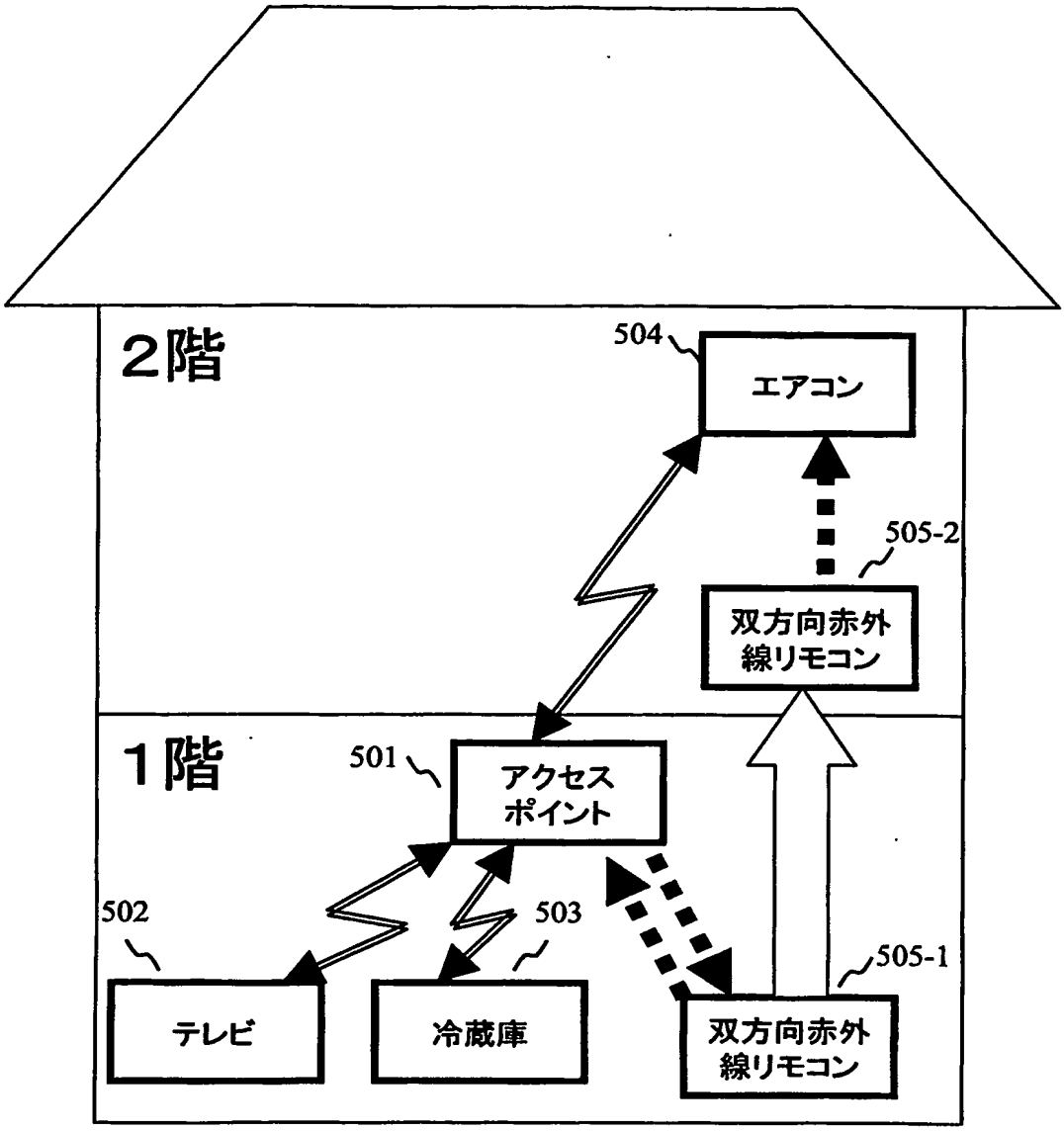
【図３】


＜第1の無線通信装置＞
104
200
無線データ利用手段
登録情報記憶手段
103
暗号手段
認証手段
101
無線通信手段
102
112
無線通信手段
113
暗号手段
認証手段
111
114
無線データ利用手段
登録情報記憶手段
210
＜第2の無線通信装置＞

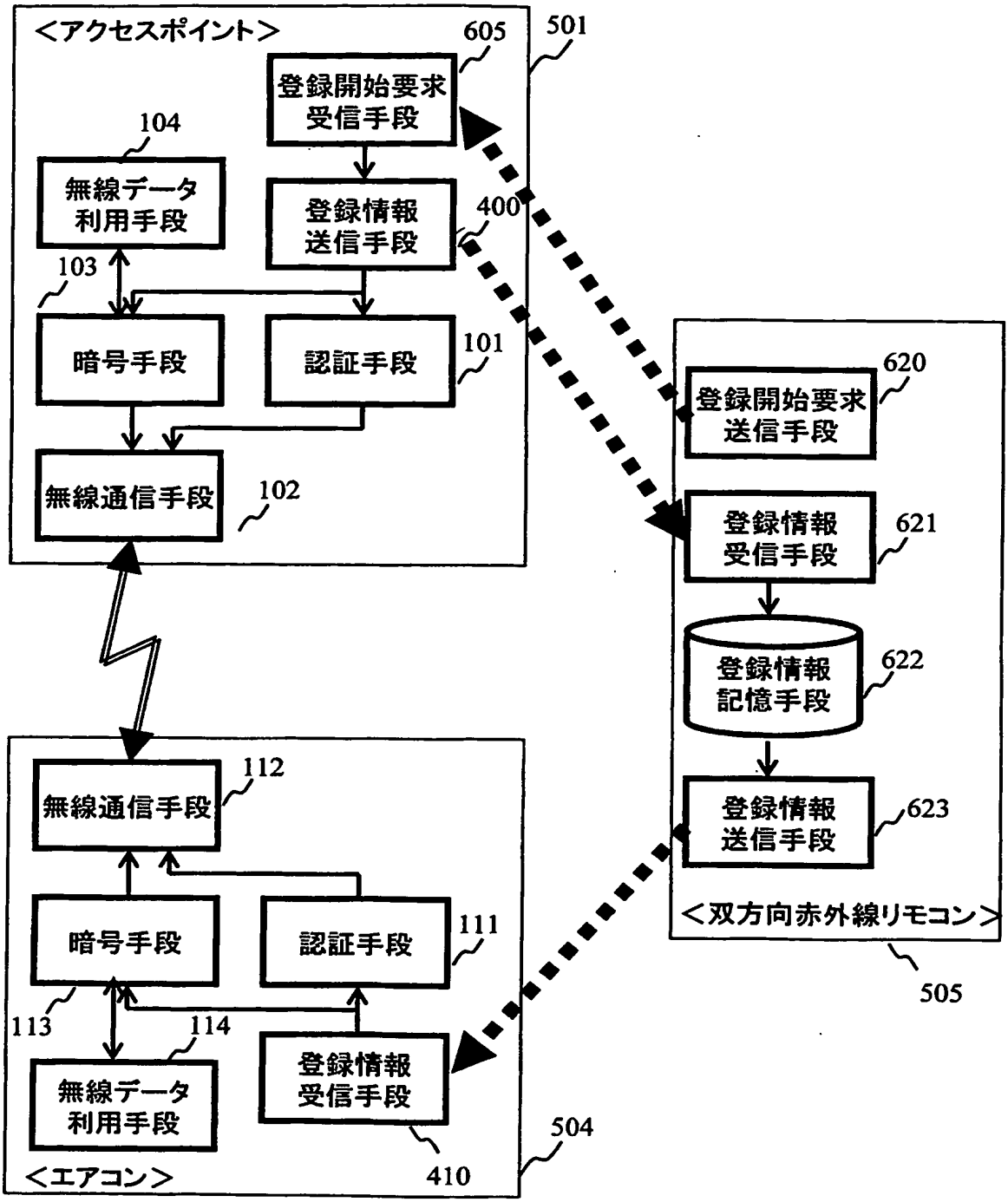
【図４】


<第1の無線通信装置>
104
無線データ利用手段
400
登録情報送信手段
103
101
暗号手段
認証手段
無線通信手段
102
112
無線通信手段
暗号手段
認証手段
111
113
114
無線データ利用手段
登録情報受信手段
410
<第2の無線通信装置>

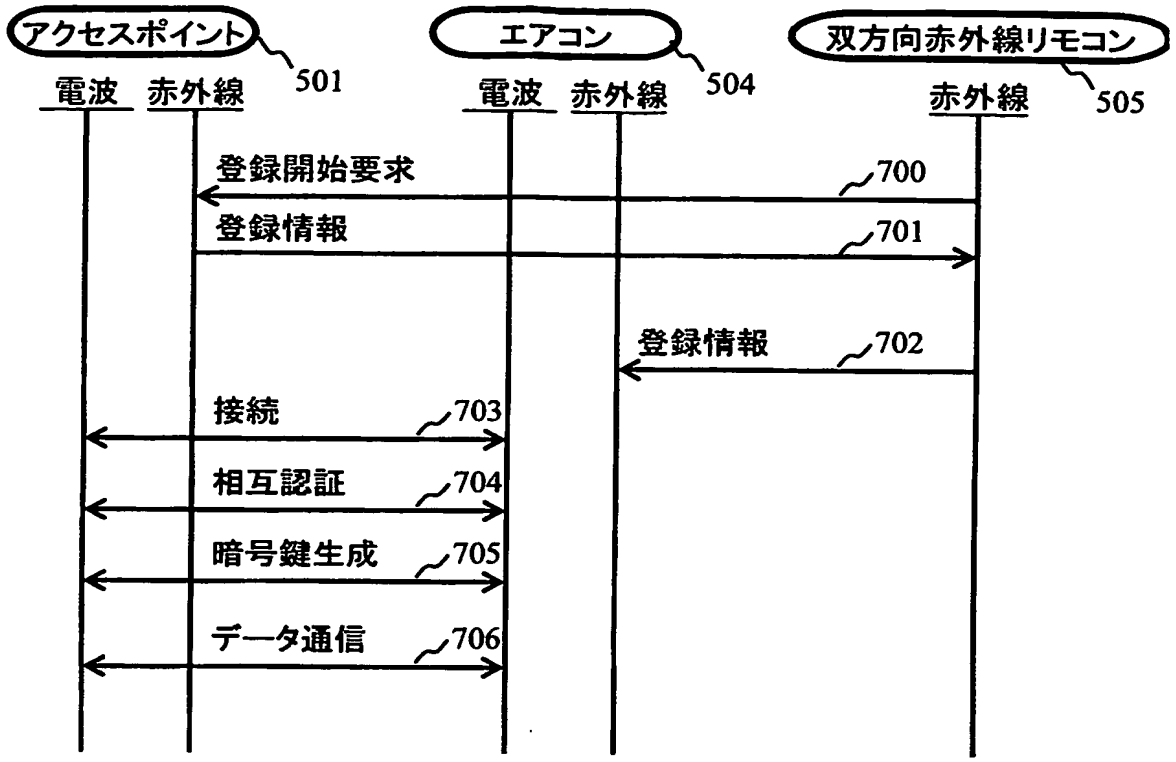
【図５】


2階
504
エアコン
505-2
双方向赤外線リモコン
1階
501
アクセスポイント
502
503
505-1
テレビ
冷蔵庫
双方向赤外線リモコン

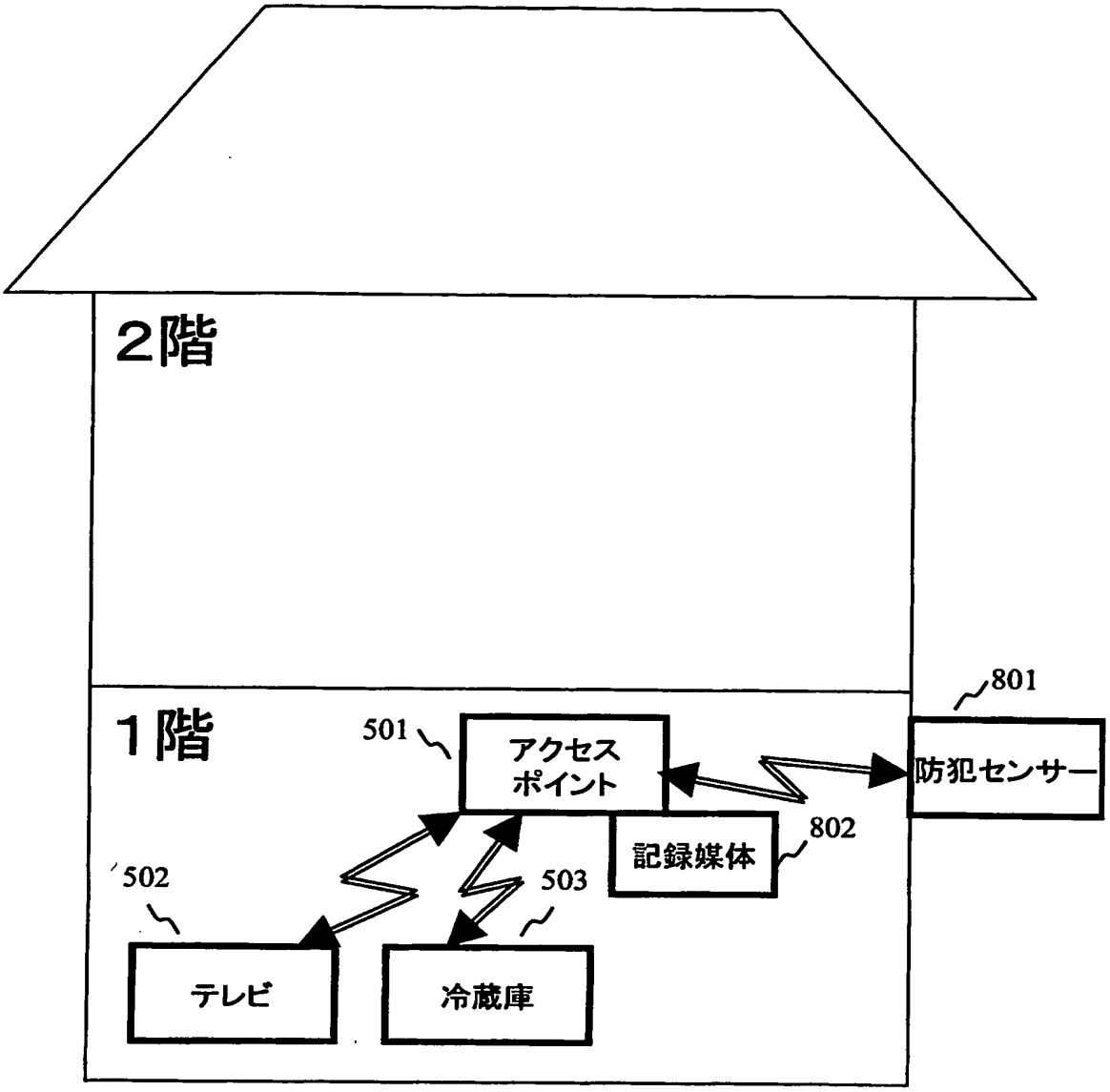
【図６】


<アクセスポイント>
605
501
登録開始要求
受信手段
104
無線データ
利用手段
登録情報
送信手段
400
103
暗号手段
認証手段
101
無線通信手段
102
620
登録開始要求
送信手段
登録情報
受信手段
621
登録情報
記憶手段
622
登録情報
送信手段
623
<双方向赤外線リモコン>
505
112
無線通信手段
暗号手段
認証手段
111
113
114
無線データ
利用手段
登録情報
受信手段
410
504
<エアコン>

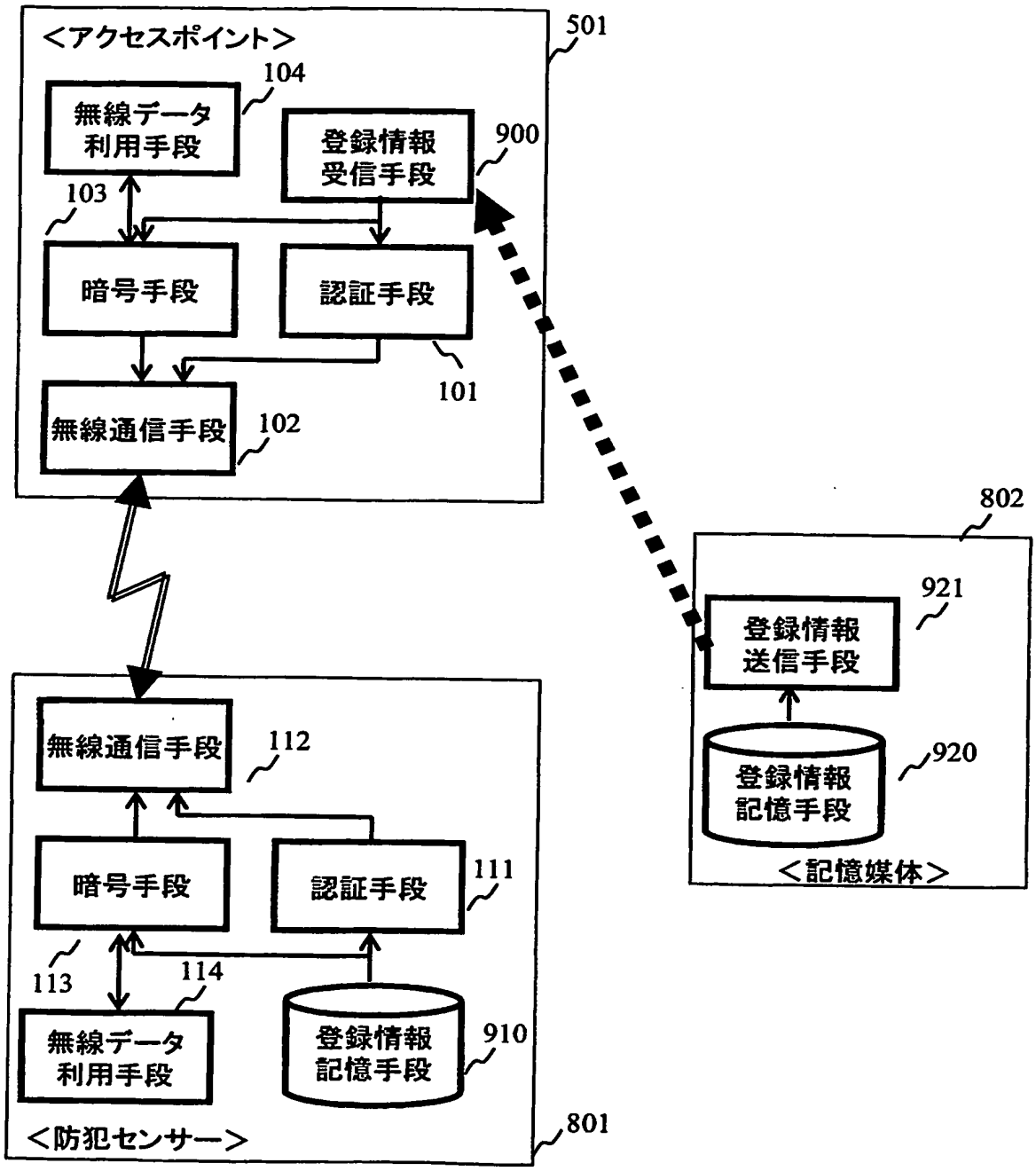
【図７】


アクセスポイント
501
電波
赤外線
エアコン
504
電波
赤外線
双方向赤外線リモコン
505
赤外線
登録開始要求
700
登録情報
701
登録情報
702
接続
703
相互認証
704
暗号鍵生成
705
データ通信
706

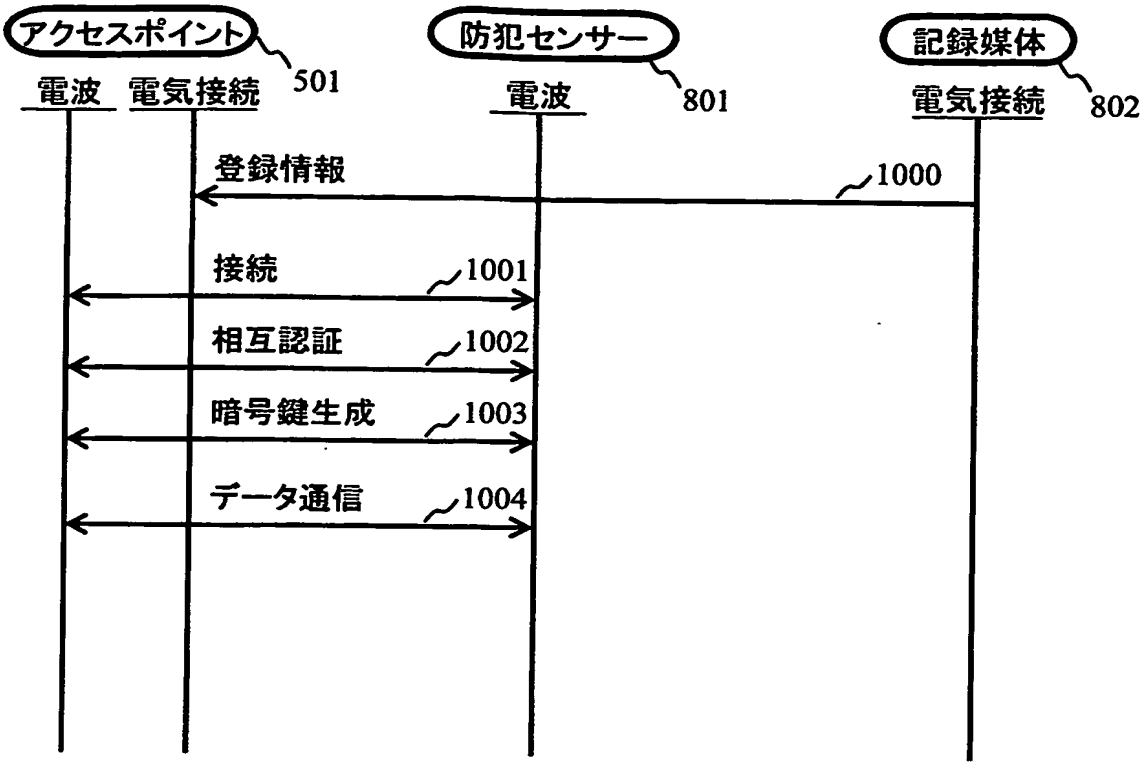
【図８】



【図９】


<アクセスポイント>
501
104
無線データ利用手段
登録情報受信手段
900
103
暗号手段
認証手段
101
無線通信手段
102
802
921
登録情報送信手段
920
登録情報記憶手段
<記憶媒体>
無線通信手段
112
暗号手段
認証手段
111
113
114
無線データ利用手段
登録情報記憶手段
910
<防犯センサー>
801

【図１０】


アクセスポイント
501
電波
電気接続
防犯センサー
801
電波
記録媒体
802
電気接続
登録情報
1000
接続
1001
相互認証
1002
暗号鍵生成
1003
データ通信
1004

【書類名】　要約書

【要約】

【課題】　本発明は、離れた場所に設置した通信装置間で、簡易に、しかも安価に互いの通信装置に関する情報を登録することを目的としている。

【解決手段】　本来の通信路（無線）よりも信頼性の高い通信路（赤外線）を利用して、機器登録の情報を通信する登録情報通信装置（双方向赤外線リモコン５０５や記憶媒体８０２）を使用して、離れた場所に設置した通信装置（アクセスポイント５０１，エアコン５０４や防犯センサー８０１）に、共有鍵を設定する。

【選択図】　図６

認定・付加情報

特許出願の番号	特願２００３－１５９９８９
受付番号	５０３００９３８１６９
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　６月　５日

＜認定情報・付加情報＞

【提出日】　平成15年 6月 4日

次頁無

特願２００３－１５９９８９

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社